UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/705,998	11/03/2000	Charanjit Singh Jutla	YOR920000763US1	4946

7590 02/24/2004

Louis P. Herzberg
Intellectual Property Law Dept.
IBM Corporation
P.O. Box 218
Yorktown Heights, NY 10598

EXAMINER	
BETIT, JACOB F	

ART UNIT	PAPER NUMBER
2175	3

DATE MAILED: 02/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/705,998	JUTLA, CHARANJIT SINGH	
	Examiner	Art Unit	
	Jacob F. Betit	2175	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03 November 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

SAM RIMELL
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 2.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Drawings

1. Figures 1-3 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Specification

2. The abstract of the disclosure is objected to because of the following informalities:

Abstract contains more than 150 words. Correction is required.

3. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

4. The arrangement of the disclosed application does not conform with 37 CFR 1.77(b).

Section headings are boldfaced throughout the disclosed specification. Section headings should not be underlined and/or **boldfaced**. Appropriate corrections are required.

Claim Objections

5. Claim 42 is objected to because of the following informalities:

Claim 42 does not end in a period. Each claim should begin with a capital letter and end with a period. Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claim 32 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. In lines 10-11 it is unclear how "dividing said cipher-text message into a plurality of cipher-text blocks" would "form an encryption of said plain text message". The specification does not show this in such a way as to enable "dividing said cipher-text message into a

plurality of cipher-text blocks to form an encryption of said plan-text message".

Appropriate correction is required.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-6, 8, 10-12, 22-23, 26, 28, 30, 33, 35, 37, 39, and 41-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Furuya et al. (European patent application publication No. 1 063 811 A1) in view of Takahashi (U.S. patent No. 5,570,307).

As to claim 1, Furuya et al. teaches a method for encrypting a plain-text message (see page 2, lines 1-3), the method comprising:

further expanding a randomness of said first random number and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers (see page 7, line 54 through page 8, line 10);

dividing said plain-text message into a plurality of plain-text blocks (see figure 15);

encrypting said plain-text blocks to form a plurality of cipher-text blocks (see page 5, lines 31-38);

combining said plurality of plain-text blocks into at least one check sum (see figure 6); and

employing said set of pair-wise differentially-uniform pseudo random numbers, together with said first random number and/or said first pseudo random number, to embed a message integrity check in said cipher-text blocks (see page 5, lines 39-43).

Furuya et al. does not teach generating a first random number; and transforming said first random number into a first pseudo random number.

Takahashi teaches generating a first random number (see column 3, lines 4-13); and transforming said first random number into a first pseudo random number (see column 3, lines 14-29).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. to include generating a first random number; and transforming said first random number into a first pseudo random number.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. by the teachings of Takahashi because generating a first random number; and transforming said first random number into a first pseudo random number would expand the random stream from the random number generator (see Takahashi, column 3, lines 14-20).

As to claim 2, Furuya et al. as modified, teaches wherein the step of encrypting said plain-text blocks includes employing the said first random number, and/or said first

pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers (see Furuya et al., column 5, lines 31-38).

As to claim 3, Furuya et al. as modified, teaches wherein the step of employing includes pairing said first random number, and/or said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, with said plurality of cipher-text blocks; and combining each pair to form a plurality of output blocks (see Furuya et al., figure 15).

As to claim 4, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing an exclusive-or operation upon components of said each pair (see Furuya et al., figure 15).

As to claim 5, Furuya et al. as modified, teaches wherein the step of encrypting includes encrypting said first random number (see Furuya et al., figure 15, where "random number" can be read on "IV", see page 6, line 53).

As to claim 6, Furuya et al. as modified, teaches wherein the step of encrypting includes encrypting said check sum (see Furuya et al., figure 6).

As to claim 8, Furuya et al. as modified, teaches wherein the step of transforming said random number includes a non-cryptographic or linear operation (see Takahashi,

column 3, lines 14-29).

As to claim 10, Furuya et al. as modified, teaches wherein the said set of pair-wise differentially-uniform numbers are set of pair-wise differentially-uniform numbers in GFp (see Furuya et al., page 7, line 54 through page 8, line 10).

As to claim 11, Furuya et al. as modified, teaches wherein the step of employing includes:

pairing said first random number, and/or said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, with said plurality of plain-text blocks; and combining each pair to form a plurality of input blocks used in said step of encrypting (see Furuya et al., figure 15).

As to claim 12, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing an exclusive-or operation upon components of said each pair (see Furuya et al., figure 15).

As to claim 22, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing a modulo p addition upon components of each said pair, wherein p is a prime number (see Furuya et al., page 5, lines 49-56).

As to claim 23, Furuya et al. as modified, teaches wherein the step of combining

each pair includes performing a modulo p addition upon components of each said pair, wherein p is a prime number (see Furuya et al., page 5, lines 49-56 and see page 7, lines 38-47).

As to claim 26, Furuya et al. as modified, teaches an article of manufacture (see Furuya et al., page 2, lines 3-5) comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 1 above).

As to claim 28, Furuya et al. as modified, teaches a computer program product (see Furuya et al., page 2, lines 3-5) comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 1 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 1 above).

As to claim 30, Furuya et al. as modified, teaches a program storage device readable by machine (see Furuya et al., page 2, lines 3-5), tangibly embodying a

program of instructions executable by the machine to perform method steps for encrypting a plain-text message, said method steps comprising the steps of claim 1 (see Furuya et al., page 2, lines 3-5).

As to claim 33, Furuya et al. teaches an apparatus to encrypt a plain-text message (see page 2, lines 1-3), the apparatus comprising:

a Pairwise Additively Uniform Sequence Generator to further expand a randomness of said first random number and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers (see page 5, line 54 through page 8, line 10);

an Encryptor to divide said plain-text message into a plurality of plain-text blocks (see figure 15), and to encrypt said plain-text blocks to form a plurality of cipher-text blocks (see page 5, lines 31-38);

a Checksum Generator to combine said plurality of plain-text blocks into at least one check sum (see figure 6); and

an Integrity Extractor and Checker to employ said set of pair-wise differentially-uniform pseudo random numbers, together with said first random number and/or said first pseudo random number, to embed a message integrity check in said cipher-text blocks (see page 5, lines 39-43).

Furuya et al. does not teach a Randomness Generator to generate a first random number; and a Randomness Transformer to transform said first random number into a first pseudo random number.

Takahashi teaches a Randomness Generator to generate a first random number (see column 3, lines 4-13); and a Randomness Transformer to transform said first random number into a first pseudo random number (see column 3, lines 14-29).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. to include a Randomness Generator to generate a first random number; and a Randomness Transformer to transform said first random number into a first pseudo random number.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. by the teachings of Takahashi because a Randomness Generator to generate a first random number; and a Randomness Transformer to transform said first random number into a first pseudo random number would expand the random stream from the random number generator (see Takahashi, column 3, lines 14-20).

As to claim 35, Furuya et al. as modified, teaches an article of manufacture (see Furuya et al., page 2, lines 3-5) comprising a Computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 2 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 2 above).

As to claim 37, Furuya et al. as modified, teaches a computer program product (see Furuya et al., page 2, lines 3-5) comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 2 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 2 above).

As to claim 39, Furuya et al. as modified, teaches a program storage device readable by machine (see Furuya et al., page 2, lines 3-5), tangibly embodying a program of instructions executable by the machine to perform method steps for encrypting a plain-text message, said method steps comprising the steps of claim 2 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 2 above).

As to claim 41, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing an addition in a group upon components of said each pair (see Furuya et al., figure 15).

As to claim 42, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing an addition in a group upon components of said each pair (see Furuya et al., figure 15).

10. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Furuya et al. (European patent application publication No. 1 063 811 A1) in view of Takahashi (U.S. patent No. 5,570,307) as applied to claims 1-6, 8, 10-12, 22-23, 26, 28, 30, 33, 35, 37, 39, and 41-42 above, and further in view of Cane et al., (U.S. patent No. 5,940,507).

As to claim 7, Furuya et al. as modified, still does not teach wherein the step of combining includes obtaining said check sum from an exclusive-or of said plurality of plain-text blocks.

Cane et al. teaches wherein the step of combining includes obtaining said check sum from an exclusive-or of said plurality of plain-text blocks (see column 4, lines 4-15).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, to include wherein the step of combining includes obtaining said check sum from an exclusive-or of said plurality of plain-text blocks.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, by the teachings of Cane et al. because wherein the step of combining includes obtaining said check sum from an exclusive-or of said plurality of plain-text blocks would provide authentication and verification of the data (see Cane et al., column 4, lines 4-15).

11. Claim 9 is rejected under 35 U.S.C. 103 (a) as being unpatentable over Furuya et

al. (European patent application publication No. 1 063 811 A1) in view of Takahashi (U.S. patent No. 5,570,307) as applied to claims 1-6, 8, 10-12, 22-23, 26, 28, 30, 33, 35, 37, 39, and 41-42 above, and further in view of Hardy et al. (U.S. patent No. 5,195,136).

As to claim 9, Furuya et al. as modified, still does not teach wherein the step of transforming said random number includes a cryptographic operation.

Hardy et al. teaches wherein the step of transforming said random number includes a cryptographic operation (see column 4, line 67 through column 5, line 21).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, to include wherein the step of transforming said random number includes a cryptographic operation.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, by the teachings of Hardy et al. because wherein the step of transforming said random number includes a cryptographic operation would produce a traffic key that could be added to a text bit stream to produce cipher text (see Hardy et al., column 5, lines 10-21).

12. Claims 13-15, 18-21, 24-25, 27, 29, 31, 34, 36, 38, 40, 43-45 rejected under 35 U.S.C. 103(a) as being unpatentable over Furuya et al. (European patent application publication No. 1 063 811 A1) in view of Brandman (U.S. patent No. 5,974,144).

As to claim 13, Furuya et al. teaches a method for decrypting a cipher-text message (see page 2, lines 3-5), the method comprising:

dividing said cipher-text message into a plurality of cipher-text blocks (see page 7, lines 43-47);

decrypting said cipher-text blocks in forming a plurality of plain-text blocks (see page 7, lines 43-50);

further expanding at least one of said plain-text blocks and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers (see figure 21);

combining said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, and/or said at least one plain-text block to form at least two check sums (see page 5, lines 25-26 and see lines 39-43) and to form a plurality of output blocks (see page 7, lines 48-50); and

comparing said at least two check sums in declaring success of a message integrity check (see page 5, lines 25-26 and see lines 39-43).

Furuya et al. does not teach transforming at least one of said plain-text blocks into a first pseudo random number.

Brandman teaches transforming at least one of said plain-text blocks into a first pseudo random number (see column 5, lines 6-34).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. to include transforming at least one of said plain-text blocks into a first pseudo random number.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. by the teachings of Brandman because transforming at least one of said plain-text blocks into a first pseudo random number would allow the user to use the random number to unscramble the second portion of data (see Brandman, column 5, lines 18-22).

As to claim 14, Furuya et al. as modified, teaches wherein the step of decrypting said cipher-text blocks includes employing said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers (see Furuya et al., page 7, lines 43-50).

As to claim 15, Furuya et al. as modified, teaches wherein the step of combining includes:

pairing said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, with said plurality of plain-text blocks (see Furuya et al., figure 8); and

using each pair to form a plurality of output blocks and employing the output blocks to form said at least two check sums (see Furuya et al., page 5, lines 25-26, and see lines 39-43).

As to claim 18, Furuya et al. as modified, teaches wherein the step of transforming said plain-text blocks includes a non-cryptographic or linear operation (see

Brandman, figure 3).

As to claim 19, Furuya et al. as modified, teaches wherein the step of transforming said plain-text blocks includes a cryptographic operation (see Brandman, column 5, lines 6-34).

As to claim 20, Furuya et al. as modified, teaches wherein the said set of pair-wise differentially-uniform numbers are set of pair-wise differentially-uniform numbers in GFp (see Furuya et al., page 7, line 54 through page 8, line 10).

As to claim 21, Furuya et al. as modified, teaches wherein the step of employing includes:

pairing said first random number, and/or said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, with said plurality of cipher-text blocks; and combining each pair to form a plurality of input blocks used in said step of decrypting (see Furuya et al., page 7, lines 43-50).

As to claim 24, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing a modulo p addition upon components of each said pair, wherein p is a prime number (see Furuya et al., page 5, lines 49-56 and see page 7, lines 38-47).

As to claim 25, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing a modulo p addition upon components of each said pair, wherein p is a prime number (see Furuya et al., page 5, lines 49-56 and see page 7, lines 38-47).

As to claim 27, Furuya et al. as modified, teaches an article of manufacture (see Furuya et al., page 2, lines 3-5) comprising a computer usable medium having computer readable program code means embodied therein for causing decryption of a cipher-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 13 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 13 above).

As to claim 29, Furuya et al. as modified, teaches a computer program product (see Furuya et al., page 2, lines 3-5) comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 13 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 13 above).

As to claim 31, Furuya et al. as modified, teaches a program storage device

readable by machine (see Furuya et al., page 2, lines 3-5), tangibly embodying a program of instructions executable by the machine to perform method steps for encrypting a plain-text message, said method steps comprising the steps of claim 13 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 13 above).

As to claim 34, Furuya et al. teaches an apparatus to decrypt a cipher-text message (see page 2, lines 3-5), the apparatus comprising:

a Decryptor to divide said cipher-text message into a plurality of cipher-text blocks (see page 7, lines 43-47), and to decrypt said cipher-text blocks in forming a plurality of plain-text blocks (see page 7, lines 43-50);

a Pairwise Additively Uniform Sequence Generator to further expand at least one of said plain-text blocks and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers (see figure 21);

a Checksum Generator to combine said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, and/or said at least one plain-text block to form at least two check sums (see page 5, lines 25-26 and see lines 39-43) and to form a plurality of output blocks (see page 7, lines 48-50); and

an Integrity Extractor and Checker to compare said at least two check sums in declaring success of a message integrity check (see column 5, lines 25-26 and see lines 39-43).

Furuya et al. does not teach a Randomness Transformer to transform at least

one of said plain-text blocks into a first pseudo random number.

Brandman teaches a Randomness Transformer to transform at least one of said plain-text blocks into a first pseudo random number (see column 5, lines 6-34).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. to include a Randomness Transformer to transform at least one of said plain-text blocks into a first pseudo random number.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. by the teachings of Brandman because a Randomness Transformer to transform at least one of said plain-text blocks into a first pseudo random number would allow the user to use the random number to unscramble the second portion of data (see Brandman, column 5, lines 18-22).

As to claim 36, Furuya et al. as modified, teaches an article of manufacture (see Furuya et al., page 2, lines 3-5) comprising a Computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 14 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 14 above).

As to claim 38, Furuya et al. as modified, teaches a computer program product

(see Furuya et al., page 2, lines 3-5) comprising a computer usable medium having computer readable program code means embodied therein for causing encryption of a plain-text message, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 14 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 14 above).

As to claim 40, Furuya et al. as modified, teaches a program storage device readable by machine (see Furuya et al., page 2, lines 3-5), tangibly embodying a program of instructions executable by the machine to perform method steps for encrypting a plain-text message, said method steps comprising the steps of claim 14 (for the teachings of this claim, the applicant is kindly directed to the remarks and discussions made in claim 14 above).

As to claim 43, Furuya et al. as modified, teaches wherein the step of using each pair includes performing an addition in a group upon components of said each pair (see Furuya et al., page 7, lines 43-50).

As to claim 44, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing an exclusive-or operation upon components of said each pair (see Furuya et al., page 7, lines 43-50).

As to claim 45, Furuya et al. as modified, teaches wherein the step of combining each pair includes performing an addition in a group upon components of said each pair (see Furuya et al., page 7, lines 43-50).

13. Claim 16 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Furuya et al. (European patent application publication No. 1 063 811 A1) in view of Brandman (U.S. patent No. 5,974,144) as applied to claims 13-15, 18-21, 24-25, 27, 29, 31, 34, 36, 38, 40, 43-45 above, and further in view of Cane et al., (U.S. patent No. 5,940,507).

As to claim 16, Furuya et al. as modified, still does not teach wherein the step of using each pair includes performing an exclusive-or operation upon components of said each pair.

Cane et al. teaches wherein the step of using each pair includes performing an exclusive-or operation upon components of said each pair (see column 4, lines 4-15).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, to include wherein the step of using each pair includes performing an exclusive-or operation upon components of said each pair.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, by the teachings of Cane et al. because wherein the step of using each pair includes performing an

exclusive-or operation upon components of said each pair would provide authentication and verification of the data (see Cane et al., column 4, lines 4-15).

As to claim 17, Furuya et al. as modified, still does not teach wherein the step of forming includes:

dividing the said output blocks into at least two subsets, and

obtaining said at least two checksums from an exclusive-or of said subsets of output blocks.

Cane et al. teaches wherein the step of forming includes: dividing the said output blocks into at least two subsets, and obtaining said at least two checksums from an exclusive-or of said subsets of output blocks (see column 4, lines 4-15).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, to include wherein the step of forming includes: dividing the said output blocks into at least two subsets, and

obtaining said at least two checksums from an exclusive-or of said subsets of output blocks.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, by the teachings of Cane et al. because wherein the step of forming includes: dividing the said output blocks into at least two subsets, and obtaining said at least two checksums from an

exclusive-or of said subsets of output blocks would provide authentication and verification of the data (see Cane et al., column 4, lines 4-15).

14. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Furuya et al. (European patent application publication No. 1 063 811 A1) in view of Takahashi (U.S. patent No. 5,570,307), and further in view of Brandman (U.S. patent No. 5,974,144).

As to claim 32, Furuya et al. teaches a method for encryption/decryption of a plain-text message (see page 2, lines 1-3), the method comprising the steps of:

further expanding a randomness of said first random number and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers (see page 7, line 54 through page 8, line 10);

dividing the plain-text message into a plurality of plain-text blocks (see figure 15);

encrypting said plain-text blocks in forming a plurality of cipher-text blocks (see page 5, lines 31-38);

combining said plurality of plain-text blocks into at least one check sum (see figure 6); and

employing said first random number, said first pseudo random number and said set of pair-wise differentially-uniform pseudo random numbers to embed a message integrity check in said cipher-text blocks to form a cipher-text message (see page 5, lines 39-43); and

dividing said cipher-text message into a plurality of cipher-text blocks to form an encryption of said plain-text message;

decrypting said cipher-text blocks in forming a plurality of plain-text blocks (see page 7, lines 43-50);

further expanding at least one of said plain-text blocks and/or said first pseudo random number into a set of pair-wise differentially-uniform pseudo random numbers (see figure 21);

combining said first pseudo random number, and/or said set of pair-wise differentially-uniform pseudo random numbers, and/or said at least one plain-text block to form at least two check sums (see page 5, lines 25-26 and see lines 39-43) and to re-form the said plain-text message (see page 7, lines 48-50); and

comparing said at least two check sums in declaring success of a message integrity check in decryption of said cipher-text to reform said plain-text message (see page 5, lines 25-26 and see lines 39-43).

Furuya et al. does not teach generating a first random number; and transforming said first random number into a first pseudo random number.

Takahashi teaches generating a first random number (see column 3, lines 4-13); and transforming said first random number into a first pseudo random number (see column 3, lines 14-29).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. to include generating a first random number; and transforming said first random number into a first pseudo

random number.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. by the teachings of Takahashi because generating a first random number; and transforming said first random number into a first pseudo random number would expand the random stream from the random number generator (see Takahashi, column 3, lines 14-20).

Furuya et al. as modified, still does not teach transforming at least one of said plain-text blocks into a first pseudo random number.

Brandman teaches transforming at least one of said plain-text blocks into a first pseudo random number (see column 5, lines 6-34).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, to include transforming at least one of said plain-text blocks into a first pseudo random number.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Furuya et al. as modified, by the teachings of Brandman because transforming at least one of said plain-text blocks into a first pseudo random number would allow the user to use the random number to unscramble the second portion of data (see Brandman, column 5, lines 18-22).

Conclusion

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob F. Betit whose telephone number is (703) 305-3735. The examiner can normally be reached on Monday through Friday 9 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dov Popovici can be reached on (703) 305-3830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

jfb
February 13, 2004

SAM RIMELL
PRIMARY EXAMINER